United Nations Office for Disarmament Affairs

Opening plenary keynote remarks at the Singapore International Cyber Week "Shaping the Next Era of Global Cybersecurity"

Izumi Nakamitsu
High Representative for Disarmament Affairs

As delivered

21 October 2025
Singapore

Honorable Minister K. Shanmugam,

Honorable Minister Teo,

Mr. Koh, Commissioner of Cybersecurity,

Excellencies,

Distinguished participants,

I am truly honoured to be here for the milestone 10th edition of Singapore International Cyber Week (SICW).

Let me begin by extending heartfelt congratulations to the Government of Singapore for this tremendous achievement!

Ten years of sustained leadership on cyber diplomacy is no small feat.

There is indeed much to commend Singapore for.

SICW has grown into a banner platform for cyber diplomacy, and Singapore remains at the forefront of international cybersecurity discussions both at the United Nations and through its regional and subregional efforts, such as those with ASEAN.

I am also very pleased that the partnership between my Office and the Cyber Security Agency of Singapore remains very strong.

I warmly welcome the extension of our joint activities, under the umbrella of the UN-Singapore Cyber Programme, for another three years. I am deeply grateful to Singapore for our partnership.

And of course, Singapore's chairing of the UN Open-ended Working Group on ICT security has been universally applauded.

I join many others in expressing deep appreciation to His Excellency Ambassador Burhan Gafoor for his exemplary efforts in leading the Working Group to a successful conclusion.

Yet, we know that the international peace and security of the ICT domain cannot be secured by the efforts of one State, one subregion, or one region, alone.

This is a collective endeavor in which we all have a role to play—from governments to individual citizens.

This is why the theme of this year's SICW— "Shaping the Next Era of Global Cybersecurity" – is so relevant.

Shaping this new era in a manner that provides for a peaceful, secure, inclusive and prosperous future is the responsibility of all of us.

This is precisely why the multistakeholder nature of this event is also so crucial, bringing together policymakers, technical experts, industry leaders, academics and many more.

Excellencies,

Distinguished participants,

Looking ahead to this "New Era of Global Cybersecurity", I would like to reflect briefly on three aspects—the role of the United Nations; the impact of advances in technology, specifically artificial intelligence; and stakeholder engagement.

First, on the role of the United Nations.

On its 80th anniversary, the United Nations' relevance, effectiveness and legitimacy are under the spotlight.

The Secretary-General has launched the UN80 Initiative to make the UN more agile, integrated and effective—essentially better equipped to respond to today's global challenges, including emerging and dynamic challenges.

ICT security falls squarely in this basket of challenges.

But while addressing these fast-moving issues is not easy, we know that States' consistent engagement at the United Nations makes a difference.

In December last year, the General Assembly adopted the Convention against Cybercrime, which creates an unprecedented platform for international cooperation in combatting crimes committed by means of ICTs.

I congratulate Viet Nam and all States on the Signing Ceremony to take place later this week in Hanoi.

Steady intergovernmental work on ICT security over more than two decades has further proven the value of dedicated engagement of Member States at the United Nations.

These discussions hit a high point in July this year when the Open-ended Working Group on ICT security adopted a consensus final report.

This marked the conclusion of four years of dedicated efforts, with notable outcomes such as:

- A global intergovernmental directory with the participation of more than 115 States so far.

- Eight global confidence-building measures to enhance trust and predictability between States, reducing tensions and misunderstandings.

- Common understandings on the ICT security threat landscape—from critical infrastructure vulnerabilities to incidents involving malicious software.

- And a whole range of capacity-building initiatives, including the convening of the first-ever Global Roundtable discussion.

And, perhaps most importantly, States agreed to establish a new Global Mechanism on ICT security to begin its work in 2026.

I believe this new process, permanent in nature, will play a crucial role in shaping our “New Era of Global Cybersecurity”.

Through annual plenary meetings and dedicated thematic groups, the Global Mechanism will be a key vehicle for States’ efforts moving forward.
We know the threats to cyberspace will not diminish, so neither can our commitment to engage.

Second, and this is connected to threats, I would like to address the impact of emerging technologies on ICT security.

If we are to talk about the future, we must acknowledge the transformative impact of rapidly advancing technologies, such as AI and quantum technology

I will speak specifically about AI, which has demonstrated itself to be among the most impactful technologies in recent history.

And, as is the case with most dual-use technologies, when it comes to AI, we are presented with both risks and opportunities.

On the one hand, the convergence of AI with ICTs is creating new vectors for exploitation and revealing novel vulnerabilities.

Integration of AI can create new ICT threats *and* significantly strengthen existing ones by increasing their speed, frequency, scale, sophistication and effect.

AI can generate malicious codes, identify system-level vulnerabilities, and spread mis-and-disinformation.

AI can also break existing encryption methods, many of which are foundational to the security of critical infrastructure systems.

But AI models can also be the subject of malicious ICT activity themselves. Perpetrators can target AI models to access source code or datasets or to inject false or misleading data into training datasets, also known as “data poisoning”.

At the same time, we must also acknowledge the potential benefits that AI can offer.

States and private companies are increasingly using AI to detect potential threats and support ICT incident response.

AI-enabled systems can automatically detect and block malicious activity, like phishing attempts and malware, analyzing quickly and efficiently unusual patterns and anomalies in network traffic.

In this way, AI can be expected to play a growing role in bolstering cyber resilience.

Thus, the "New Era of Global Cybersecurity" will require careful consideration of AI and its enabling role—both from the point of view of the perpetrator and also defender.

Third and finally, allow me a few words on engagement of stakeholders.

I have said many times before that the role of non-governmental stakeholders in ICT-related discussions cannot be overstated.

When it comes to cybersecurity, we all have a stake—which makes all of us stakeholders in some manner.

The very nature of ICTs—with much of their infrastructure owned and operated across borders and by a range of stakeholders—requires close and multi-sectoral collaboration.

From States to the business community, to technical experts to scholars, there is a multitude of roles to play.

Stakeholder roles include operating and defending infrastructure, providing practical guidance on the implementation of norms and the application of international law, conducting capacity building activities, and gathering and sharing threat intelligence.

This is just to name a few.

Particularly when it comes to examining the impact of emerging technologies on cybersecurity, we must engage the private sector that is largely driving this innovation forward.

While multi-stakeholder processes introduce more complexity, I must say, they also provide for increased opportunity.

Let us seize this opportunity together.

Excellencies,

Distinguished participants,

I look forward to joining forces in “Shaping the Next Era of Global Cybersecurity”, both this week at SICW and in the days and months ahead.

Rest assured that the United Nations is your committed partner.

I thank very much you for your attention.